

Policy 20

CCTV Policy 2026/2027

This policy applies to all members of our workforce, visitors and all other persons whose images may be captured by the CCTV system.

20.1 Purpose of CCTV

20.1.1 Reach uses CCTV for the following purposes:

- To provide a safe and secure environment for pupils, staff and visitors
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

20.2 Description of System

20.2.1 Reach buildings can have a number of cameras both inside and outside. Cameras are of the fixed type and do not include sound recording

20.3 Siting of Cameras

20.3.1 All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.

20.3.2 Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. Reach will make all reasonable efforts to ensure that areas outside of the premises and grounds are not recorded.

20.3.3 Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

20.3.4 Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets.

20.4 Privacy Impact Assessment

20.4.1 Prior to the installation or repositioning of any CCTV camera, or system, a privacy impact assessment will be conducted by Reach to ensure that the proposed installation is compliant with legislation and ICO guidance. The assessment will be approved by the Director.

20.4.2 Reach will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

20.5 Management and Access

20.5.1 The CCTV system will be managed by a member of the Leadership Team.

20.5.2 Any allegations against staff will be referred immediately to the Director and only they will determine who needs to view the footage. Allegations against the Director will be referred to the Local Authority Designated Officer (LADO).

20.5.3 On a day-to-day basis the CCTV system will be operated by an individual with appropriate technical ability. This will be the individual running the Duty desk.

20.5.4 The viewing of live CCTV images will be restricted (with the exception of live CCTV positioned in external public areas) to the Leadership Team, site management team, IT management team and others delegated by the Leadership Team. In doing so they will ensure that the Purposes of CCTV are satisfied.

20.5.5 Recorded images which are stored by the CCTV system will be restricted by the same principles of live imagery. Relevant images may be shared for disciplinary matters and complaints.

20.5.6 No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.

20.5.7 The CCTV system is checked daily to ensure that it is operating effectively

20.6 Storage and Retention of Images

20.6.1 Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.

20.6.2 Recorded images are stored for a maximum of 7 days unless there is a specific purpose for which they are retained for a longer period.

20.6.3 Reach will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

- CCTV recording systems being located in restricted access areas
- The CCTV system being encrypted/password protected
- Restriction of the ability to make copies to specified members of staff
- A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the Reach

20.7 Disclosure of Images to Data Subject

20.7.1 Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has a right to request access to those images

20.7.2 Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation.

20.7.3 When such a request is made the appropriate individual with access to the CCTV footage will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.

20.7.4 If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The individual accessing the footage must take appropriate measures to ensure that the footage is restricted in this way.

20.7.5 If the footage contains images of other individuals, then Reach must consider whether:

- The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;
- The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

20.7.6 If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

A record must be kept, and held securely, of all disclosures which sets out:

- When the request was made;
- The process followed by the individual with access to the CCTV footage in determining whether the images contained third parties;
- The considerations as to whether to allow access to those images;
- The individuals that were permitted to view the images and when;
- Whether a copy of the images was provided, and if so to whom, when and in what format

20.8 Disclosure of Images to Third Parties

20.8.1 Reach will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

20.8.2 CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

20.8.3 If a request is received from a law enforcement agency for disclosure of CCTV images, then the individual with access to the CCTV footage must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third-party images.

20.8.4 The information above must be recorded in relation to any disclosure.

20.8.5 If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

20.9 Misuse of CCTV systems

20.9.1 The misuse of CCTV system could constitute a criminal offence.

20.9.2 Any member of staff who breaches this policy may be subject to disciplinary action.

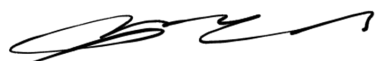
20.10 Complaints relating to this policy

20.10.1 Any complaints relating to this policy or to the CCTV system operated by Reach should be made in accordance with company policy.

Any further questions regarding guidelines in this policy then please contact one of the leadership team.

To ensure the effectiveness of this document our 'CCTV' policy will be reviewed annually.

Signed:



Date: 2nd Sept 2026

Dan Palmer

Founder / Director